

ISOMORPHISM OF COMPLETE LOCAL NOETHERIAN RINGS AND STRONG APPROXIMATION

LOU VAN DEN DRIES

(Communicated by Bernd Ulrich)

ABSTRACT. About a year ago Angus Macintyre raised the following question. Let A and B be complete local noetherian rings with maximal ideals \mathfrak{m} and \mathfrak{n} such that A/\mathfrak{m}^n is isomorphic to B/\mathfrak{n}^n for every n . Does it follow that A and B are isomorphic? We show that the answer is *yes* if the residue field is algebraic over its prime field. The proof uses a strong approximation theorem of Pfister and Popescu, or rather a variant of it, which we obtain by a method due to Denef and Lipshitz. Examples by Gabber show that the answer is *no* in general.

1. INTRODUCTION

Throughout, d, e, m, n, μ, ν range over $\mathbb{N} = \{0, 1, 2, \dots\}$ and rings are assumed to be commutative with 1. Given a local ring A with maximal ideal \mathfrak{m} we put $A_n := A/\mathfrak{m}^n$. Unless specified otherwise, isomorphisms are ring isomorphisms. Given rings A, B , we let $\text{Iso}(A, B)$ be the set of isomorphisms $A \rightarrow B$.

Recall, for example from [3], that a complete local noetherian ring is isomorphic to $\mathbf{k}[[x_1, \dots, x_d]]/I$ or to $V[[x_1, \dots, x_d]]/I$, where \mathbf{k} is a field, V is a complete DVR, x_1, \dots, x_d are distinct indeterminates, and I is an ideal of $\mathbf{k}[[x_1, \dots, x_d]]$, respectively, $V[[x_1, \dots, x_d]]$. Here “DVR” abbreviates “discrete valuation ring”.

Let A and B be complete local noetherian rings with maximal ideals \mathfrak{m} and \mathfrak{n} . Note: if $A_n \cong B_n$ for all n , then A and B have isomorphic residue fields A/\mathfrak{m} and B/\mathfrak{n} , and A and B have the same Hilbert function

$$n \mapsto \dim_{A/\mathfrak{m}} \mathfrak{m}^n/\mathfrak{m}^{n+1} = \dim_{B/\mathfrak{n}} \mathfrak{n}^n/\mathfrak{n}^{n+1},$$

and so equal Krull dimension and embedding dimension. Inspired by a claim in a preprint by Schoutens, Angus Macintyre asked:

Question. Suppose $A_n \cong B_n$ for all n . Does it follow that $A \cong B$?

If A is regular with a subfield, then we have a positive answer because A and B have the same Hilbert function; see [3]. Cutkosky mentioned to me that [1] yields a positive answer when A and B are reduced, equicharacteristic, equidimensional formal germs of isolated singularities. The main result of the present paper is a positive answer when the residue field is algebraic:

Received by the editors December 18, 2006, and, in revised form, September 4, 2007.

2000 *Mathematics Subject Classification.* Primary 13B40, 13J10; Secondary 13L05.

Key words and phrases. Complete local noetherian ring, strong approximation.

©2008 American Mathematical Society
Reverts to public domain 28 years from publication

Theorem 1.1. *Suppose that $A_n \cong B_n$ for all n , and the residue field A/\mathfrak{m} is algebraic over its prime field. Then $A \cong B$.*

After a talk I gave on this result (Paris, January 2007), Ofer Gabber came up with examples where Macintyre's question has a negative answer. These examples are presented at the end of the paper, with thanks to Gabber.

We begin with a simple fact that gives the theorem for finite residue fields. Assume that $A_n \cong B_n$ for all n . Each isomorphism $A_{n+1} \rightarrow B_{n+1}$ induces an isomorphism $A_n \rightarrow B_n$, so we have for each n a natural map

$$\text{Iso}(A_{n+1}, B_{n+1}) \rightarrow \text{Iso}(A_n, B_n),$$

giving an inverse system $(\text{Iso}(A_n, B_n))_n$ of *nonempty* sets. We now observe:

Fact. The question has a positive answer if and only if the inverse limit of this system of sets is nonempty.

For example, if the residue field A_1 is finite, then all A_n are finite, hence all sets $\text{Iso}(A_n, B_n)$ are finite and nonempty, and so their inverse limit is nonempty. Thus the question has a positive answer if A has finite residue field.

If we assume a common coefficient field for A and B and allow only isomorphisms that are the identity on this coefficient field, the question also has a positive answer: this is shown in section 2 to be a consequence of a known strong approximation property for power series rings over fields. For the original question this gives a positive answer when the residue field is a number field as we show in section 3, but it doesn't suffice when the residue field is algebraic of infinite degree over its prime field. To handle that, we need a variant of strong approximation where we allow an automorphism of the coefficient field as an extra unknown in the equations figuring in the approximation property. In section 4 we obtain this variant as in Denef-Lipshitz [2], and then use this to prove the theorem above in the equicharacteristic case, that is, the case where A has a subfield. In sections 5 and 6 we deal with the mixed characteristic case using Witt vectors and the Teichmüller map.

In proving the theorem we try to lift an isomorphism $A_m \rightarrow B_m$ to an isomorphism $A \rightarrow B$. The next lemma shows that it is enough to do this for $m = 2$ and to lift to a local morphism rather than an isomorphism. (A *local morphism* from a local ring R into a local ring R' is a ring morphism $R \rightarrow R'$ that maps the maximal ideal of R into the maximal ideal of R' .)

Lemma 1.2. *Let A be a complete local noetherian ring and ϕ a local endomorphism of A inducing the identity on A_2 . Then ϕ is an automorphism.*

Proof. We have $\phi = 1 - \theta$, where 1 is the identity map on A and $\theta : A \rightarrow A$ is additive. The assumption on ϕ yields that $\theta(A) \subseteq \mathfrak{m}^2$, where \mathfrak{m} is the maximal ideal of A . We claim that $\theta(\mathfrak{m}^n) \subseteq \mathfrak{m}^{n+1}$ for all $n \geq 1$. To see this, let $n \geq 1$ and $a_1, \dots, a_n \in \mathfrak{m}$; then

$$\begin{aligned} a_1 \cdots a_n - \theta(a_1 \cdots a_n) &= \phi(a_1 \cdots a_n) = \phi(a_1) \cdots \phi(a_n) \\ &= (a_1 - \theta(a_1)) \cdots (a_n - \theta(a_n)) \in a_1 \cdots a_n + \mathfrak{m}^{n+1}, \end{aligned}$$

so $\theta(a_1 \cdots a_n) \in \mathfrak{m}^{n+1}$. This proves the claim. It follows that $\theta^n(A) \subseteq \mathfrak{m}^{n+1}$ for all $n \geq 1$, and so we have a two-sided inverse $1 + \theta + \theta^2 + \cdots : A \rightarrow A$ of ϕ . \square

We also need the following *uniqueness* of lifting residue fields:

Lemma 1.3. *Let R be a henselian local ring, let $\pi : R \rightarrow \mathbf{k}$ be a ring morphism onto a field \mathbf{k} that is separably-algebraic over a subfield \mathbf{k}_0 , and let $\iota_0 : \mathbf{k}_0 \rightarrow R$ be a ring morphism such that $\pi \circ \iota_0 = \text{id}_{\mathbf{k}_0}$. Then ι_0 has a unique extension to a ring morphism $\iota : \mathbf{k} \rightarrow R$ such that $\pi \circ \iota = \text{id}_{\mathbf{k}}$.*

Proof. Given any $\alpha \in \mathbf{k}$, take its minimal polynomial $f(T)$ over \mathbf{k}_0 . Then $f'(\alpha) \neq 0$. Let $g(T) \in R[T]$ be the image of $f(T) \in \mathbf{k}_0[T]$ under ι_0 . Since R is henselian we have a unique $a \in R$ such that $g(a) = 0$ and $\pi(a) = \alpha$, and thus ι_0 has a unique extension to a ring morphism $\iota_\alpha : \mathbf{k}_0(\alpha) \rightarrow R$ such that $\pi \circ \iota_\alpha = \text{id}_{\mathbf{k}_0(\alpha)}$. \square

Further notational conventions. Let R be a ring and I a proper ideal of R . For $r = (r_1, \dots, r_n) \in R^n$ and $s = (s_1, \dots, s_n) \in R^n$ we write $r \equiv s \pmod{I}$ to indicate that $r_i \equiv s_i \pmod{I}$ for $i = 1, \dots, n$. Recall that the ideal I^n of R is generated by the products $a_1 \cdots a_n$ with $a_1, \dots, a_n \in I$. To avoid confusion with this ideal we indicate the cartesian product

$$I \times \cdots \times I := \{(a_1, \dots, a_n) : a_1, \dots, a_n \in I\} \subseteq R^n$$

by IR^n . For a map $f : X \rightarrow Y$ and $(a_1, \dots, a_n) \in X^n$ we put

$$f(a) := (f(a_1), \dots, f(a_n)) \in Y^n.$$

Given $r = (r_1, \dots, r_n) \in R^n$ and $i = (i_1, \dots, i_n) \in \mathbb{N}^n$ we also use the multinomial notation $r^i := r_1^{i_1} \cdots r_n^{i_n} \in R$, and put $|i| := i_1 + \cdots + i_n$.

2. STRONG APPROXIMATION AND LIFTING MORPHISMS

Let R be a complete local noetherian ring with maximal ideal \mathfrak{m} . We say that R has the *strong approximation property* if for all $K, M, N \in \mathbb{N}$ and

$$f_1, \dots, f_K \in R[[Z]][[U]], \quad Z = (Z_1, \dots, Z_M), \quad U = (U_1, \dots, U_N),$$

with distinct indeterminates $Z_1, \dots, Z_M, U_1, \dots, U_N$, and for any $\mu > 0$ there is a $\nu > \mu$ with the following property: for all $z = (z_1, \dots, z_M) \in \mathfrak{m}R^M$ and all $u = (u_1, \dots, u_N) \in R^N$ such that

$$f_k(z, u) \equiv 0 \pmod{\mathfrak{m}^\nu} \quad \text{for } k = 1, \dots, K,$$

there are $z' = (z'_1, \dots, z'_M) \in \mathfrak{m}R^M$ and $u' = (u'_1, \dots, u'_N) \in R^N$ such that

$$(z', u') \equiv (z, u) \pmod{\mathfrak{m}^\mu} \quad \text{and } f_k(z', u') = 0 \quad \text{for } k = 1, \dots, K.$$

A result by Pfister and Popescu [4] says that power series rings $\mathbf{k}[[y_1, \dots, y_e]]$ over fields \mathbf{k} have the strong approximation property. See Denef and Lipshitz [2] for a nice proof using an Artin-type approximation theorem for Weierstrass systems, and ultraproducts. We are going to use this strong approximation property to deduce a lifting property of morphisms between complete local noetherian rings with a given coefficient field.

In the rest of this section \mathbf{k} is a field and A and B are complete local noetherian \mathbf{k} -algebras, with maximal ideals \mathfrak{m} and \mathfrak{n} , respectively, such that the natural maps $\mathbf{k} \rightarrow A \rightarrow A/\mathfrak{m}$ and $\mathbf{k} \rightarrow B \rightarrow B/\mathfrak{n}$ of \mathbf{k} into the residue fields are surjective. We consider $A_n := A/\mathfrak{m}^n$ and $B_n := B/\mathfrak{n}^n$ as \mathbf{k} -algebras in the usual way, and all morphisms $A \rightarrow B$ and $A_n \rightarrow B_n$ are assumed to be \mathbf{k} -algebra morphisms and thus local morphisms.

Proposition 2.1. *For any $m > 0$, there is an $n > m$ (depending on m, A , and B) such that any morphism $A_m \rightarrow B_m$ that can be lifted to a morphism $A_n \rightarrow B_n$ can be lifted to a morphism $A \rightarrow B$.*

Proof. We can assume $A = \mathbf{k}[[x]]/I$ and $B = \mathbf{k}[[y]]/J$ with ideals $I = (f_1, \dots, f_k) \subseteq (x)\mathbf{k}[[x]]$ and $J = (g_1, \dots, g_l) \subseteq (y)\mathbf{k}[[y]]$ with $x = x_1, \dots, x_d$ and $y = y_1, \dots, y_e$ and where $x_1, \dots, x_d, y_1, \dots, y_e$ are distinct power series variables.

A morphism $\phi : A \rightarrow B$ is completely determined by the tuple

$$\phi(x_1 + I), \dots, \phi(x_d + I).$$

Here we use “morphism” in this section to mean a “ \mathbf{k} -algebra morphism”, not just a “local morphism”. Conversely, let any $z_1, \dots, z_d \in (y)\mathbf{k}[[y]]$ be given. Then there is a morphism $\phi : A \rightarrow B$ such that $\phi(x_1 + I) = z_1 + J, \dots, \phi(x_d + I) = z_d + J$, if and only if $f_1(z_1, \dots, z_d), \dots, f_k(z_1, \dots, z_d) \in J$, which in turn is equivalent to the solvability in the ring $\mathbf{k}[[y]]$ of the equations

$$\begin{aligned} f_1(z_1, \dots, z_d) &= u_{11}g_1 + \dots + u_{1l}g_l \\ \dots &= \dots \\ \dots &= \dots \\ f_k(z_1, \dots, z_d) &= u_{k1}g_1 + \dots + u_{kl}g_l \end{aligned}$$

in the unknowns u_{11}, \dots, u_{kl} . Thus the morphisms $A \rightarrow B$ come from solutions in $\mathbf{k}[[y]]$ of the above system of equations where now z_1, \dots, z_d are also considered as unknowns, ranging only over the maximal ideal $(y)\mathbf{k}[[y]]$ of $\mathbf{k}[[y]]$. Likewise, for each $n > 0$ the morphisms $A_n \rightarrow B_n$ come from solutions modulo $(y)^n$ in $\mathbf{k}[[y]]$ of the above system of equations, with the same restriction on z_1, \dots, z_d . Here “modulo $(y)^n$ ” means that the equality signs of the system are to be read as “is congruent modulo $(y)^n$ to”. The strong approximation property of the ring $\mathbf{k}[[y]]$ now yields the desired result. □

Corollary 2.2. *There is an $n > 0$, depending on A and B , such that if A_n and B_n are isomorphic, then A and B are isomorphic.*

Proof. Take $n > 2$ as in the proposition for $m = 2$, such that n works not only for the pair A, B but also for the pair B, A . Suppose $\phi_n : A_n \rightarrow B_n$ is an isomorphism, and let $\phi_2 : A_2 \rightarrow B_2$ be the induced isomorphism. By the proposition we can lift ϕ_2 to a morphism $\phi : A \rightarrow B$, and we can lift the inverse of ϕ_2 to a morphism $\psi : B \rightarrow A$. Then $\psi \circ \phi$ is an endomorphism of A inducing the identity on A_2 , so is an automorphism of A by Lemma 1.2. Likewise, $\phi \circ \psi$ is an automorphism of B . Thus ϕ is an isomorphism. □

Krupinski pointed out to me that for $A = \mathbf{k}[[x, y]]/(y^2)$ (with distinct indeterminates x and y), each A_n with $n \geq 3$ has an automorphism that cannot be lifted to an endomorphism of A_{n+1} . In particular, the corollary above cannot be improved to say that there is an integer $n > 0$ such that any isomorphism $A_n \rightarrow B_n$ lifts to an isomorphism $A \rightarrow B$.

3. THE CASE WHERE THE RESIDUE FIELD IS A NUMBER FIELD

We now return to the setting of the introduction, so A and B are complete local noetherian rings with maximal ideals \mathfrak{m} and \mathfrak{n} . We shall now use Corollary 2.2 to obtain the following special case of the main theorem, Theorem 1.1.

Corollary 3.1. *Suppose $A_n \cong B_n$ for all n , and A/\mathfrak{m} is algebraic over its prime field and has only finitely many automorphisms. Then $A \cong B$.*

Proof. We already have this in the positive residue characteristic case, where the assumption on the residue field means that the residue field is finite. For the rest of the proof we can therefore assume that A and B contain \mathbb{Q} as a subfield. The assumption on automorphisms gives us an isomorphism $i : A/\mathfrak{m} \rightarrow B/\mathfrak{n}$ that can be lifted for every $n > 0$ to an isomorphism $A_n \rightarrow B_n$. Identify $\mathbf{k} = A/\mathfrak{m}$ with B/\mathfrak{n} via i . Let $\pi_A : A \rightarrow \mathbf{k}$ and $\pi_B : B \rightarrow \mathbf{k}$ be the canonical maps. With $\mathbf{k} \supseteq \mathbb{Q}$ and $\mathbf{k}_0 = \mathbb{Q}$, Lemma 1.3 yields unique ring morphisms $\iota_A : \mathbf{k} \rightarrow A$ and $\iota_B : \mathbf{k} \rightarrow B$ such that $\pi_A \circ \iota_A = \text{id}_{\mathbf{k}}$ and $\pi_B \circ \iota_B = \text{id}_{\mathbf{k}}$. Construe A and B as \mathbf{k} -algebras via ι_A and ι_B ; as quotients of A and B this makes A_n and B_n into \mathbf{k} -algebras. Let $n > 0$ and take a ring isomorphism $\phi_n : A_n \rightarrow B_n$ that induces the identity on $\mathbf{k} = A/\mathfrak{m} = B/\mathfrak{n}$. We claim that ϕ_n is a \mathbf{k} -algebra isomorphism. To see this, let $\pi_{A,n} : A \rightarrow A_n$ and $\pi_{B,n} : B \rightarrow B_n$ be the canonical maps. The claim amounts to the equality

$$\phi_n \circ \pi_{A,n} \circ \iota_A = \pi_{B,n} \circ \iota_B.$$

This equality follows by Lemma 1.3 applied to $R = B_n$ by noting that both maps composed on the left with the natural map $B_n \rightarrow \mathbf{k} = B/\mathfrak{n}$ are equal to $\text{id}_{\mathbf{k}}$.

It now follows from Corollary 2.2 that A and B are isomorphic as \mathbf{k} -algebras; in particular, they are isomorphic as rings. \square

This yields Theorem 1.1 for the case that A/\mathfrak{m} is isomorphic to a number field, or to

$$\mathbb{Q}_p^{\text{alg}} := \{x \in \mathbb{Q}_p : x \text{ is algebraic over } \mathbb{Q}\} \quad (p \text{ any prime number}),$$

or to the field of real algebraic numbers. In the next section we show how to handle the case that A contains a field and A/\mathfrak{m} is any algebraic extension of its prime field, for example an algebraic closure of its prime field.

4. STRONG APPROXIMATION WITH AUTOMORPHISMS

Here we prove Theorem 1.1 in the equicharacteristic case. For this we shall use a version of strong approximation that allows automorphisms. The approach of [2] can easily be adapted to give this version. For the convenience of the reader we give the details, modulo the Artin-type approximation theorem for W-systems (Weierstrass systems) from [2]. (A W-system over a field \mathbf{k} is a family (R_n) , each R_n a \mathbf{k} -subalgebra of $\mathbf{k}[[X_1, \dots, X_n]]$, such that certain axioms are satisfied, the main one being closure under Weierstrass division; here X_1, X_2, X_3, \dots are distinct indeterminates.)

Let $y_1, \dots, y_e, Z_1, \dots, Z_M, U_1, \dots, U_N$ be distinct indeterminates, $M, N \in \mathbb{N}$,

$$y = (y_1, \dots, y_e), \quad Z = (Z_1, \dots, Z_M), \quad U = (U_1, \dots, U_N), \quad R := \mathbf{k}[[y]],$$

so $\mathfrak{m} := (y_1, \dots, y_e)R$ is the maximal ideal of R . We let i, α , and β range over \mathbb{N}^e , \mathbb{N}^M , and \mathbb{N}^N , respectively, and for

$$f = f(Z, U) = \sum_{i, \alpha, \beta} c_{i\alpha\beta} y^i Z^\alpha U^\beta \in R[[Z]][U] = \mathbf{k}[[y, Z]][U] \subseteq \mathbf{k}[[y, Z, U]],$$

with coefficients $c_{i\alpha\beta} \in \mathbf{k}$ for all i, α, β , and with $\sigma \in \text{Aut}(\mathbf{k})$ we put

$$\sigma f := \sum_{i, \alpha, \beta} \sigma(c_{i\alpha\beta}) y^i Z^\alpha U^\beta \in R[[Z]][U].$$

So $\text{Aut}(\mathbf{k})$ acts by automorphisms on the ring $R[[Z]][U]$ via $(\sigma, f) \mapsto \sigma f$.

We now assume \mathbf{k} is algebraic over a given subfield \mathbf{k}_0 of \mathbf{k} , and put

$$G := \{\sigma \in \text{Aut}(\mathbf{k}) : \sigma \text{ is the identity on } \mathbf{k}_0\}.$$

In particular, $G(c) := \{\sigma(c) : \sigma \in G\}$ is finite for each $c \in \mathbf{k}$. We can now state a strong approximation property with automorphisms from G . Its proof follows closely that of Theorem 7.1 in [2].

Proposition 4.1. *Let $K \in \mathbb{N}$, $f_1, \dots, f_K, g_1, \dots, g_K \in R[[Z]][U]$ and $\mu \in \mathbb{N}$. Then there is a natural number $\nu > \mu$ with the following property: if $z = (z_1, \dots, z_M) \in \mathfrak{m}R^M$, $u = (u_1, \dots, u_N) \in R^N$, and $\sigma \in G$ are such that*

$$(\sigma f_k)(z, u) \equiv g_k(z, u) \pmod{\mathfrak{m}^\nu} \quad \text{for } k = 1, \dots, K,$$

then there are $z' = (z'_1, \dots, z'_M) \in \mathfrak{m}R^M$ and $u' = (u'_1, \dots, u'_N) \in R^N$ and $\sigma' \in G$ such that

$$(z', u') \equiv (z, u) \pmod{\mathfrak{m}^\mu}, \quad (\sigma' f_k)(z', u') = g_k(z', u'), \quad \text{for } k = 1, \dots, K.$$

Proof. Take a nonprincipal ultrafilter D on \mathbb{N} and put $R^* = R^\mathbb{N}/D$, an elementary extension R^* of R with maximal ideal \mathfrak{m}^* and subfield $\mathbf{k}^* = \mathbf{k}^\mathbb{N}/D$. Note that \mathbf{k}^* has \mathbf{k} as a subfield. We let j range over \mathbb{N} , and for a sequence (a_j) in R we put $[a_j] := (a_j)/D \in R^*$. Any sequence (σ_j) in G yields an automorphism σ^* of \mathbf{k}^* by

$$\sigma^*([c_j]) := [\sigma_j(c_j)] \quad (\text{all } c_j \in \mathbf{k}).$$

Then $\sigma^*(\mathbf{k}) = \mathbf{k}$ with $\sigma^*|_{\mathbf{k}} \in G$, since \mathbf{k} is algebraic over \mathbf{k}_0 . Such a σ^* will be called an *internal automorphism* of \mathbf{k}^* . Given $f(Z, U) \in R[[Z]][U]$ we have the map

$$(z, u) \mapsto f(z, u) : \mathfrak{m}R^M \times R^N \rightarrow R,$$

which extends in the usual way to a map

$$(z^*, u^*) \mapsto f(z^*, u^*) : \mathfrak{m}^*(R^*)^M \times (R^*)^N \rightarrow R^*.$$

Also, when an internal automorphism σ^* of \mathbf{k}^* is given by a sequence (σ_j) in G as above, we define $\sigma^* f : \mathfrak{m}^*(R^*)^M \times (R^*)^N \rightarrow R^*$ by

$$(\sigma^* f)([z_{1j}], \dots, [z_{Mj}], [u_{1j}], \dots, [u_{Nj}]) = [(\sigma_j f)(z_{1j}, \dots, z_{Mj}, u_{1j}, \dots, u_{Nj})],$$

where $z_{1j}, \dots, z_{Mj} \in \mathfrak{m}$, $u_{1j}, \dots, u_{Nj} \in R$ for all j .

Let $\pi : R^* \rightarrow \mathbf{k}^*[[y]]$ be the (surjective) \mathbf{k}^* -algebra morphism given by

$$\pi \left[\sum_i c_{ij} y^i \right] := \sum_i [c_{ij}] y^i \quad (\text{all } c_{ij} \in \mathbf{k}).$$

It is clear that π is the identity on the common subring R of R^* and $\mathbf{k}^*[[y]]$; hence the maximal ideal $(y_1, \dots, y_e)\mathbf{k}^*[[y]]$ of $\mathbf{k}^*[[y]]$ is equal to $\pi\mathfrak{m}^*$. Therefore,

$$\pi^{-1}((\pi\mathfrak{m}^*)^n) = (\mathfrak{m}^*)^n \text{ for all } n, \text{ and thus}$$

$$\mathbf{k}\pi = (\mathfrak{m}^*)^\infty := \bigcap_n (\mathfrak{m}^*)^n.$$

Let $f(Z, U) \in R[[Z]][U]$, $z^* \in \mathfrak{m}^*(R^*)^M$, $u^* \in (R^*)^N$, and let σ^* be an internal automorphism of \mathbf{k}^* , and put $\sigma := \sigma^*|_{\mathbf{k}}$, so $\sigma \in G$. Then

$$\pi((\sigma^* f)(z^*, u^*)) = (\sigma f)(\pi z^*, \pi u^*).$$

This is routine to check for $f \in \mathbf{k}[y, Z, U]$ and then follows easily for general f .

Suppose there is no $\nu > \mu$ as claimed by the proposition. Take for each $\nu > \mu$ a counterexample to obtain tuples $z^* = (z_1^*, \dots, z_M^*) \in \mathfrak{m}^*(R^*)^M$ and $u^* = (u_1^*, \dots, u_N^*) \in (R^*)^N$, and an internal automorphism σ^* of \mathbf{k}^* such that

$$(\sigma^* f_k)(z^*, u^*) \equiv g_k(z^*, u^*) \pmod{(\mathfrak{m}^*)^\infty}, \quad \text{for } k = 1, \dots, K,$$

and such that there are no $z' = (z'_1, \dots, z'_M) \in \mathfrak{m}^*(R^*)^M$ and $u' = (u'_1, \dots, u'_N) \in (R^*)^N$ and an internal automorphism σ' of \mathbf{k}^* with

$$\begin{aligned} (\sigma' f_k)(z', u') &= g_k(z', u'), \quad \text{for } k = 1, \dots, K, \\ z' &\equiv z^* \pmod{(\mathfrak{m}^*)^\mu} \quad \text{and } u' \equiv u^* \pmod{(\mathfrak{m}^*)^\mu}. \end{aligned}$$

Put $\sigma := \sigma^*|_{\mathbf{k}}$, so $\sigma \in G$. Applying π to the congruences above gives

$$(\sigma f_k)(\pi z^*, \pi u^*) = g_k(\pi z^*, \pi u^*) \text{ in } \mathbf{k}^*[[y]], \quad \text{for } k = 1, \dots, K.$$

Fix distinct indeterminates X_1, X_2, X_3, \dots , and for $X = (X_1, \dots, X_n)$, put

$$\mathbf{k}^*[X] := \bigcup \{D[[X]] \subseteq \mathbf{k}^*[[X]] : D \text{ is a finitely generated } \mathbf{k}\text{-subalgebra of } \mathbf{k}^*\}.$$

Then $(\mathbf{k}^*[X_1, \dots, X_n])_n$ is a W-system over \mathbf{k}^* by Lemma 7.2 in [2]. Let $\mathbf{k}^*[y]$ be the image of $\mathbf{k}^*[X_1, \dots, X_e]$ under the \mathbf{k}^* -algebra isomorphism

$$\mathbf{k}^*[[X_1, \dots, X_e]] \rightarrow \mathbf{k}^*[[y]], \quad X_1 \mapsto y_1, \dots, X_e \mapsto y_e.$$

Then Theorem 1.1 in [2] gives $\tilde{z} = (\tilde{z}_1, \dots, \tilde{z}_M) \in (y_1, \dots, y_e)(\mathbf{k}^*[y])^M$ and $\tilde{u} = (\tilde{u}_1, \dots, \tilde{u}_N) \in \mathbf{k}^*[y]^N$, such that in $\mathbf{k}^*[[y]]$,

$$\begin{aligned} (\sigma f_k)(\tilde{z}, \tilde{u}) &= g_k(\tilde{z}, \tilde{u}) \text{ for } k = 1, \dots, K, \\ (\tilde{z}, \tilde{u}) &\equiv (\pi z^*, \pi u^*) \pmod{(\pi \mathfrak{m}^*)^\mu}. \end{aligned}$$

Take $c = (c_1, \dots, c_s) \in (\mathbf{k}^*)^s$, $s \in \mathbb{N}$, with $\tilde{z} \in \mathbf{k}[c][[y]]^M$ and $\tilde{u} \in \mathbf{k}[c][[y]]^N$, so

$$\tilde{z} = \sum_i p_i(c)y^i, \quad \tilde{u} = \sum_i q_i(c)y^i,$$

where $p_i(T) \in \mathbf{k}[T]^M$, $q_i(T) \in \mathbf{k}[T]^N$, $T = (T_1, \dots, T_s)$, for all i , and where $p_{(0, \dots, 0)} = (0, \dots, 0)$. Then, for $k = 1, \dots, K$,

$$(\sigma f_k)(y, \sum_i p_i(c)y^i, \sum_i q_i(c)y^i) = g_k(y, \sum_i p_i(c)y^i, \sum_i q_i(c)y^i).$$

For $k = 1, \dots, K$ we have polynomials $h_{ki}(T) \in \mathbf{k}[T]$ such that in $\mathbf{k}[T][[y]]$,

$$(\sigma f_k)(y, \sum_i p_i(T)y^i, \sum_i q_i(T)y^i) - g_k(y, \sum_i p_i(T)y^i, \sum_i q_i(T)y^i) = \sum_i h_{ki}(T)y^i;$$

hence $h_{ki}(c) = 0$ for all i . Take $d > 0$ such that the ideal of $\mathbf{k}[T]$ generated by all $h_{ki}(T)$ is generated by the $h_{ki}(T)$ with $|i| < d$. Now $(c_1, \dots, c_s) = ([c_{1j}], \dots, [c_{sj}])$, where $c_{1j}, \dots, c_{sj} \in \mathbf{k}$ for all j . Put $c(j) := (c_{1j}, \dots, c_{sj}) \in \mathbf{k}^s$, and take $S \in D$ such that $h_{ki}(c(j)) = 0$ for $k = 1, \dots, K$, $|i| < d$, $j \in S$. Put

$$\begin{aligned} z(j) &= (z_1(j), \dots, z_M(j)) := \sum_i p_i(c(j))y^i \in \mathfrak{m}R^M, \\ u(j) &= (u_1(j), \dots, u_N(j)) := \sum_i q_i(c(j))y^i \in R^N, \end{aligned}$$

so $(\sigma f_k)(z(j), u(j)) = g_k(z(j), u(j))$ for $j \in S$. For $z := ([z_1(j)], \dots, [z_M(j)]) \in \mathfrak{m}^*(R^*)^M$ and $u := ([u_1(j)], \dots, [u_N(j)]) \in (R^*)^N$ this gives

$$\begin{aligned}
 (\sigma f_k)(z, u) &= g_k(z, u) \text{ for } k = 1, \dots, K, \text{ and } \pi z = \tilde{z}, \quad \pi u = \tilde{u}, \\
 \text{so } (z, u) &\equiv (z^*, u^*) \pmod{(\mathfrak{m}^*)^\mu}.
 \end{aligned}$$

This contradicts the properties of z^* and u^* stated earlier in the proof. □

In the rest of this section A and B are complete local noetherian rings with maximal ideals \mathfrak{m} and \mathfrak{n} , as before, and “morphism” will mean “ring morphism”.

Proposition 4.2. *Suppose A and B have subfields, $A/\mathfrak{m} \cong B/\mathfrak{n}$, and A/\mathfrak{m} is algebraic over its prime field. Then any morphism $A \rightarrow B$ is local, and for any $m > 0$ there is an $n > m$ such that any morphism $A_m \rightarrow B_m$ that can be lifted to a morphism $A_n \rightarrow B_n$ can be lifted to a morphism $A \rightarrow B$.*

Proof. We can assume $A = \mathbf{k}[[x]]/I$ and $B = \mathbf{k}[[y]]/J$, where \mathbf{k} is a field algebraic over its prime field and $I = (f_1, \dots, f_k) \subseteq (x)\mathbf{k}[[x]]$ and $J = (g_1, \dots, g_l) \subseteq (y)\mathbf{k}[[y]]$ are ideals, with $x = x_1, \dots, x_d$ and $y = y_1, \dots, y_e$, and where $x_1, \dots, x_d, y_1, \dots, y_e$ are distinct variables. We identify \mathbf{k} with its image in A and its image in B via the natural maps $\mathbf{k} \rightarrow \mathbf{k}[[x]] \rightarrow A$ and $\mathbf{k} \rightarrow \mathbf{k}[[y]] \rightarrow B$, and we put $G := \text{Aut}(\mathbf{k})$. Suppose $\phi : A \rightarrow B$ is a morphism. Then $\phi(\mathbf{k})$ is a subfield of B that is mapped into and hence onto B/\mathfrak{n} by the natural map $B \rightarrow B/\mathfrak{n}$. Hence $\phi(\mathbf{k}) = \mathbf{k}$, by Lemma 1.3, so ϕ is local and $\phi|_{\mathbf{k}} = \sigma$ with $\sigma \in G$. Note that $\phi : A \rightarrow B$ is completely determined by σ and $\phi(x_1 + I), \dots, \phi(x_d + I)$. Conversely, given any $\sigma \in G$ and $z_1, \dots, z_d \in (y)\mathbf{k}[[y]]$, there is a morphism $\phi : A \rightarrow B$ such that

$$\phi|_{\mathbf{k}} = \sigma \text{ and } \phi(x_1 + I) = z_1 + J, \dots, \phi(x_d + I) = z_d + J$$

if and only if $(\sigma f_1)(z_1, \dots, z_d), \dots, (\sigma f_k)(z_1, \dots, z_d) \in J$, which in turn is equivalent to the solvability in the ring $\mathbf{k}[[y]]$ of the equations

$$\begin{aligned}
 (\sigma f_1)(z_1, \dots, z_d) &= u_{11}g_1 + \dots + u_{1l}g_l \\
 \dots\dots\dots &= \dots\dots\dots \\
 \dots\dots\dots &= \dots\dots\dots \\
 (\sigma f_k)(z_1, \dots, z_d) &= u_{k1}g_1 + \dots + u_{kl}g_l
 \end{aligned}$$

in the unknowns u_{11}, \dots, u_{kl} . Thus the morphisms $A \rightarrow B$ come from solutions in G and $\mathbf{k}[[y]]$ of the above system of equations where now σ (ranging over G) and z_1, \dots, z_d (ranging over the maximal ideal $(y)\mathbf{k}[[y]]$ of $\mathbf{k}[[y]]$) are also considered as unknowns. Likewise, for each $n > 0$ the morphisms $A_n \rightarrow B_n$ come from solutions modulo $(y)^n$ in G and $\mathbf{k}[[y]]$ of the above system of equations, with the same restrictions on σ and z_1, \dots, z_d . Here “modulo $(y)^n$ ” means that the equality signs of the system are to be read as “is congruent modulo $(y)^n$ to”. Now Proposition 4.1 yields the desired result. □

In the equicharacteristic case we now remove from Corollary 3.1 the assumption that A/\mathfrak{m} has only finitely many automorphisms. The proof is the same, except that it uses Proposition 4.2 in place of Proposition 2.1.

Corollary 4.3. *Suppose A and B have subfields, $A_n \cong B_n$ for all n , and A/\mathfrak{m} is algebraic over its prime field. Then $A \cong B$.*

5. LIFTING MORPHISMS OVER COMPLETE DISCRETE VALUATION RINGS

In section 2 we considered A and B as algebras over a common coefficient field, but here we allow more general *coefficient rings*, as defined in [3].

In this section V is a complete DVR, and A and B are complete local noetherian V -algebras, with maximal ideals \mathfrak{m} and \mathfrak{n} , respectively, such that the natural maps $V \rightarrow A \rightarrow A/\mathfrak{m}$ and $V \rightarrow B \rightarrow B/\mathfrak{n}$ of V into the residue fields are surjective. We consider $A_n := A/\mathfrak{m}^n$ and $B_n := B/\mathfrak{n}^n$ as V -algebras in the usual way, so all V -algebra morphisms $A \rightarrow B$ and $A_n \rightarrow B_n$ are in particular local morphisms. It is shown in [4] and [2] that the strong approximation property also holds for power series rings $V[[y_1, \dots, y_e]]$, and as in section 2 we obtain:

Proposition 5.1. *For any $m > 0$, there is an $n > m$ (depending on m , A , and B) such that any V -algebra morphism $A_m \rightarrow B_m$ that can be lifted to a V -algebra morphism $A_n \rightarrow B_n$ can be lifted to a V -algebra morphism $A \rightarrow B$.*

The proof is the same as that of Proposition 2.1, with V instead of \mathbf{k} , and the role of the maximal ideals $(x_1, \dots, x_d)\mathbf{k}[[x]]$ and $(y_1, \dots, y_e)\mathbf{k}[[y]]$ of $\mathbf{k}[[x]]$ and $\mathbf{k}[[y]]$ is taken over by the maximal ideals $(t, x_1, \dots, x_d)V[[x]]$ and $(t, y_1, \dots, y_e)V[[y]]$ of $V[[x]]$ and $V[[y]]$; here t is a generator of the maximal ideal of V .

Corollary 5.2. *There is an $n > 0$, depending on A and B , such that if A_n and B_n are isomorphic as V -algebras, then A and B are isomorphic as V -algebras.*

Theorem 1.1 still remains to be established in the case that A does not contain a field and the residue field of A is of characteristic $p > 0$ and algebraic of infinite degree over its (finite) prime field. This is done in the next section. There we need a special case of the following construction.

Let t be a generator of the maximal ideal of V . For $s \in \mathbb{N}$ and a tuple $T = (T_1, \dots, T_s)$ of s distinct indeterminates, let $V\langle T \rangle$ be the subring of $V[[T]]$ consisting of the power series $f(T) = \sum_i a_i T^i$ (with i ranging over \mathbb{N}^s and all $a_i \in V$) such that for each n we have $a_i \in t^n V$ for all but finitely many i . In particular, $V\langle T \rangle$ is a subring of $V[[T]]$, and, as noted in Section 6 of [2], the ring $V\langle T \rangle$ is noetherian. Let W be a complete DVR with V as a subring and t in the maximal ideal of W , and let $c \in W^s$. Then we have a V -algebra morphism

$$f(T) \mapsto f(c) := \sum_i a_i c^i : V\langle T \rangle \rightarrow W$$

with $f(T)$ as above; we put $V\langle c \rangle := \{f(c) : f \in V\langle T \rangle\}$, a V -subalgebra of W .

6. THE MIXED CHARACTERISTIC CASE

In this section “morphism” means “ring morphism”. Let \mathbf{k} denote a perfect field of characteristic $p > 0$, and put $V := W[\mathbf{k}]$, the ring of Witt vectors over \mathbf{k} . The elements of V are vectors (c_0, c_1, c_2, \dots) with components $c_n \in \mathbf{k}$; see [5]. So V is a complete DVR with a canonical morphism

$$\pi_V : V \rightarrow \mathbf{k}, \quad \pi_V(c_0, c_1, c_2, \dots) := c_0 \quad (\text{all } c_n \in \mathbf{k}).$$

Thus π_V has a kernel pV , the maximal ideal of V . Each $\sigma \in \text{Aut}(\mathbf{k})$ lifts uniquely to an automorphism of the ring V , denoted also by σ , in the sense that for all $a \in V$ we have $\pi_V(\sigma a) = \sigma(\pi_V(a))$; it is given by

$$\sigma((c_0, c_1, c_2, \dots)) = (\sigma(c_0), \sigma(c_1), \sigma(c_2), \dots) \quad (\text{all } c_n \in \mathbf{k}).$$

Next we state an analogue of Proposition 4.1, with V instead of \mathbf{k} and a similar proof. Because of some possibly confusing differences we give this proof anyway, despite considerable overlap with that of Proposition 4.1.

Let $y_1, \dots, y_e, Z_1, \dots, Z_M, U_1, \dots, U_N$ be distinct indeterminates, $M, N \in \mathbb{N}$,

$$y = (y_1, \dots, y_e), \quad Z = (Z_1, \dots, Z_M), \quad U = (U_1, \dots, U_N), \quad R := V[[y]],$$

so $\mathfrak{m} := (p, y_1, \dots, y_e)R$ is the maximal ideal of R . We let i, α , and β range over $\mathbb{N}^e, \mathbb{N}^M$, and \mathbb{N}^N , respectively, and for

$$f = f(Z, U) = \sum_{i, \alpha, \beta} c_{i\alpha\beta} y^i Z^\alpha U^\beta \in R[[Z]][U] = V[[y, Z]][U] \subseteq V[[y, Z, U]],$$

with coefficients $c_{i\alpha\beta} \in V$ for all i, α, β , and with $\sigma \in \text{Aut}(\mathbf{k})$ we put

$$\sigma f := \sum_{i, \alpha, \beta} \sigma(c_{i\alpha\beta}) y^i Z^\alpha U^\beta \in R[[Z]][U].$$

So $\text{Aut}(\mathbf{k})$ acts by automorphisms on the ring $R[[Z]][U]$ via $(\sigma, f) \mapsto \sigma f$.

Assume \mathbf{k} is algebraic over a given subfield \mathbf{k}_0 of \mathbf{k} , and put

$$G := \{\sigma \in \text{Aut}(\mathbf{k}) : \sigma \text{ is the identity on } \mathbf{k}_0\}.$$

Then we have strong approximation with automorphisms from G :

Proposition 6.1. *Let $K \in \mathbb{N}$, $f_1, \dots, f_K, g_1, \dots, g_K \in R[[Z]][U]$ and $\mu \in \mathbb{N}$. Then there is a natural number $\nu > \mu$ with the following property: if $z = (z_1, \dots, z_M) \in \mathfrak{m}R^M$ and $u = (u_1, \dots, u_N) \in R^N$, and $\sigma \in G$ are such that*

$$(\sigma f_k)(z, u) \equiv g_k(z, u) \pmod{\mathfrak{m}^\nu} \quad \text{for } k = 1, \dots, K,$$

then there are $z' = (z'_1, \dots, z'_M) \in \mathfrak{m}R^M$ and $u' = (u'_1, \dots, u'_N) \in R^N$ and $\sigma' \in G$ such that

$$(z', u') \equiv (z, u) \pmod{\mathfrak{m}^\mu}, \quad (\sigma' f_k)(z', u') = g_k(z', u'), \quad \text{for } k = 1, \dots, K.$$

Proof. Take a nonprincipal ultrafilter D on \mathbb{N} and put $R^* = R^\mathbb{N}/D$, an elementary extension R^* of R with maximal ideal \mathfrak{m}^* and subring $V^* = V^\mathbb{N}/D$. Note that V^* has V as a subring. Let j range over \mathbb{N} , and for a sequence (a_j) in R , put $[a_j] := (a_j)/D \in R^*$. We have the extension field $\mathbf{k}^* := \mathbf{k}^\mathbb{N}/D$ of \mathbf{k} , and $\pi_V : V \rightarrow \mathbf{k}$ extends to the morphism

$$\pi_{V^*} : V^* \rightarrow \mathbf{k}^*, \quad \pi_{V^*}([c_j]) := [\pi_V(c_j)] \quad (\text{all } c_j \in V).$$

As in the proof of Proposition 4.1, any sequence (σ_j) in G yields an internal automorphism σ^* of \mathbf{k}^* with $\sigma^*|_{\mathbf{k}} \in G$. The sequence (σ_j) also gives an automorphism of V^* , denoted by σ^* as well and defined by $\sigma^*([c_j]) = [\sigma_j(c_j)]$ (all $c_j \in V$), so

$$\sigma^*(\pi_{V^*}(c)) = \pi_{V^*}(\sigma^*(c)) \text{ for } c \in V^*.$$

Given $f(Z, U) \in R[[Z]][U]$ we have the map

$$(z, u) \mapsto f(z, u) : \mathfrak{m}R^M \times R^N \rightarrow R,$$

which extends in the usual way to a map

$$(z^*, u^*) \mapsto f(z^*, u^*) : \mathfrak{m}^*(R^*)^M \times (R^*)^N \rightarrow R^*,$$

and also when an internal automorphism σ^* of \mathbf{k}^* is given by a sequence (σ_j) in G as above, we define $\sigma^*f : \mathfrak{m}^*(R^*)^M \times (R^*)^N \rightarrow R^*$ by

$$(\sigma^*f)([z_{1j}, \dots, [z_{Mj}], [u_{1j}, \dots, [u_{Nj}]] = [(\sigma_j f)(z_{1j}, \dots, z_{Mj}, u_{1j}, \dots, u_{Nj})],$$

where $z_{1j}, \dots, z_{Mj} \in \mathfrak{m}$, $u_{1j}, \dots, u_{Nj} \in R$ for all j .

Set $W := W[\mathbf{k}^*]$, the ring of Witt vectors over \mathbf{k}^* , so $V = W[\mathbf{k}] \subseteq W[\mathbf{k}^*] = W$. We also put

$$(p^\infty) := \bigcap_n p^n V^*, \quad V' := V^*/(p^\infty),$$

and let $\pi' : V^* \rightarrow V'$ be the canonical morphism and $\pi_{V'} : V' \rightarrow \mathbf{k}^*$ the surjective morphism such that $\pi_{V^*} = \pi_{V'} \circ \pi'$. Since V' is a complete DVR with maximal ideal pV' we have a unique isomorphism $\iota : V' \rightarrow W$ such that $\pi_W \circ \iota = \pi_{V'}$, and below we identify V' with W via ι ; this makes π' a surjective morphism $V^* \rightarrow W$ such that $\pi_{V^*} = \pi_W \circ \pi'$.

Let $\pi : R^* \rightarrow W[[y]]$ be the (surjective) V -algebra morphism defined by

$$\pi \left[\sum_i c_{ij} y^i \right] := \sum_i \pi'([c_{ij}]) y^i \quad (\text{all } c_{ij} \in V).$$

It is clear that π is the identity on the common subring R of R^* and $W[[y]]$; hence the maximal ideal $(p, y_1, \dots, y_e)W[[y]]$ of $W[[y]]$ equals $\pi\mathfrak{m}^* = (p, y_1, \dots, y_e)W[[y]]$. Therefore,

$$\pi^{-1}((\pi\mathfrak{m}^*)^n) = (\mathfrak{m}^*)^n \text{ for all } n, \text{ and thus}$$

$$\ker \pi = (\mathfrak{m}^*)^\infty := \bigcap_n (\mathfrak{m}^*)^n.$$

Let $f(Z, U) \in R[[Z]][[U]]$, $z^* \in \mathfrak{m}^*(R^*)^M$, $u^* \in (R^*)^N$, and let σ^* be an internal automorphism of \mathbf{k}^* , and put $\sigma := \sigma^*|_{\mathbf{k}}$, so $\sigma \in G$. Then

$$\pi((\sigma^*f)(z^*, u^*)) = (\sigma f)(\pi z^*, \pi u^*) \text{ in } W[[y]].$$

This is easy to check for $f \in V[y, Z, U]$ and then follows for general f .

Suppose there is no $\nu > \mu$ as claimed by the proposition. For each $\nu > \mu$ we take a counterexample, to obtain tuples $z^* = (z_1^*, \dots, z_M^*) \in \mathfrak{m}^*(R^*)^M$ and $u^* = (u_1^*, \dots, u_N^*) \in (R^*)^N$, and an internal automorphism σ^* of \mathbf{k}^* such that

$$(\sigma^*f_k)(z^*, u^*) \equiv g_k(z^*, u^*) \pmod{(\mathfrak{m}^*)^\infty}, \quad \text{for } k = 1, \dots, K,$$

and such that there are no $z' = (z'_1, \dots, z'_M) \in \mathfrak{m}^*(R^*)^M$ and $u' = (u'_1, \dots, u'_N) \in (R^*)^N$ and an internal automorphism σ' of \mathbf{k}^* with

$$(\sigma'f_k)(z', u') = g_k(z', u'), \quad \text{for } k = 1, \dots, K,$$

$$(z', u') \equiv (z^*, u^*) \pmod{(\mathfrak{m}^*)^\mu}.$$

Put $\sigma := \sigma^*|_{\mathbf{k}}$, so $\sigma \in G$. Applying π to the congruences above gives

$$(\sigma f_k)(\pi z^*, \pi u^*) = g_k(\pi z^*, \pi u^*) \text{ in } W[[y]], \quad \text{for } k = 1, \dots, K.$$

Fix distinct indeterminates X_1, X_2, X_3, \dots , and for $X = (X_1, \dots, X_n)$, put

$$W[X] := \bigcup \{V\langle c \rangle[[X]] : s \in \mathbb{N}, c \in W^s\} \subseteq W[[X]].$$

Then $(W[X_1, \dots, X_n])_n$ is a W -system over W by Lemma 7.2 in [2]. Let $W[y]$ be the image of $W[X_1, \dots, X_e]$ under the W -algebra isomorphism

$$W[[X_1, \dots, X_e]] \rightarrow W[[y]], \quad X_1 \mapsto y_1, \dots, X_e \mapsto y_e.$$

Then Theorem 1.1 in [2] gives $\tilde{z} = (\tilde{z}_1, \dots, \tilde{z}_M) \in (p, y_1, \dots, y_e)(W[y])^M$ and $\tilde{u} = (\tilde{u}_1, \dots, \tilde{u}_N) \in W[y]^N$, such that in $W[[y]]$,

$$(\sigma f_k)(\tilde{z}, \tilde{u}) = g_k(\tilde{z}, \tilde{u}) \text{ for } k = 1, \dots, K,$$

$$(\tilde{z}, \tilde{u}) \equiv (\pi z^*, \pi u^*) \pmod{(\pi \mathfrak{m}^*)^\mu}.$$

Take $c = (c_1, \dots, c_s) \in W^s$, $s \in \mathbb{N}$, with $\tilde{z} \in V\langle c \rangle[[y]]^M$ and $\tilde{u} \in V\langle c \rangle[[y]]^N$, so

$$\tilde{z} = \sum_i p_i(c)y^i, \quad \tilde{u} = \sum_i q_i(c)y^i,$$

where $p_i(T) \in V\langle T \rangle^M$, $q_i(T) \in V\langle T \rangle^N$, $T = (T_1, \dots, T_s)$, for all i . Increasing s , if necessary, we arrange that $p_{(0, \dots, 0)}(T) \in p(V\langle T \rangle)^M$. Then, for $k = 1, \dots, K$,

$$(\sigma f_k)(y, \sum_i p_i(c)y^i, \sum_i q_i(c)y^i) = g_k(y, \sum_i p_i(c)y^i, \sum_i q_i(c)y^i).$$

For $k = 1, \dots, K$ we have $h_{ki}(T) \in V\langle T \rangle$ such that in $V\langle T \rangle[[y]]$,

$$(\sigma f_k)(y, \sum_i p_i(T)y^i, \sum_i q_i(T)y^i) - g_k(y, \sum_i p_i(T)y^i, \sum_i q_i(T)y^i) = \sum_i h_{ki}(T)y^i;$$

hence $h_{ki}(c) = 0$ for all i . Take $d > 0$ such that the ideal of $V\langle T \rangle$ generated by all $h_{ki}(T)$ is generated by the $h_{ki}(T)$ with $|i| < d$. Theorem 6.1 in [2] yields a $\nu > \mu$ such that for all $a \in V^s$, if

$$h_{ki}(a) \in p^\nu V \text{ for } k = 1, \dots, K \text{ and all } i \text{ with } |i| < d,$$

then there is $b \in V^s$ such that

$$a \equiv b \pmod{p^\mu V} \text{ and } h_{ki}(b) = 0 \text{ for } k = 1, \dots, K \text{ and all } i \text{ with } |i| < d.$$

Now $c = (c_1, \dots, c_s) = (\pi'[c_{1j}], \dots, \pi'[c_{sj}])$ where $c_{1j}, \dots, c_{sj} \in V$ for all j . Put $c(j) := (c_{1j}, \dots, c_{sj}) \in V^s$. With ν as above we can take $S \in D$ such that $h_{ki}(c(j)) \in p^\nu V$ for $k = 1, \dots, K$, $|i| < d$, $j \in S$. Next, take $b(j) \in V^s$ for each j such that for $k = 1, \dots, K$, $|i| < d$, $j \in S$ we have $b(j) \equiv c(j) \pmod{p^\mu V}$ and $h_{ki}(b(j)) = 0$. Put

$$z(j) = (z_1(j), \dots, z_M(j)) := \sum_i p_i(b(j))y^i \in \mathfrak{m}R^M,$$

$$u(j) = (u_1(j), \dots, u_N(j)) := \sum_i q_i(b(j))y^i \in R^N,$$

so $(\sigma f_k)(z(j), u(j)) = g_k(z(j), u(j))$ for $j \in S$. For $z := ([z_1(j)], \dots, [z_M(j)]) \in \mathfrak{m}^*(R^*)^M$ and $u := ([u_1(j)], \dots, [u_N(j)]) \in (R^*)^N$ this gives

$$(\sigma f_k)(z, u) = g_k(z, u) \text{ for } k = 1, \dots, K, \text{ and } (\pi z, \pi u) \equiv (\tilde{z}, \tilde{u}) \pmod{p^\mu W[[y]]},$$

$$\text{so } (z, u) \equiv (z^*, u^*) \pmod{(\mathfrak{m}^*)^\mu}.$$

This contradicts the properties of z^* and u^* stated earlier in the proof. □

The proper ideals of V are $\{0\}$ and the $p^n V$ with $n > 0$. For each proper ideal I of V we have the morphisms $\pi_I : V \rightarrow V/I$ and $\pi_{V/I} : V/I \rightarrow \mathfrak{k}$ such that $\pi_I(a) = a + I$ for all $a \in V$ and $\pi_V = \pi_{V/I} \circ \pi_I$.

Let I and J be proper ideals of V and $\phi : V/I \rightarrow V/J$ a morphism. Then $I \subseteq J$, and ϕ induces an endomorphism σ of \mathfrak{k} in the sense that the diagram

$$\begin{array}{ccc}
 V/I & \xrightarrow{\phi} & V/J \\
 \pi_{V/I} \downarrow & & \downarrow \pi_{V/J} \\
 \mathbf{k} & \xrightarrow{\sigma} & \mathbf{k}
 \end{array}$$

commutes. Note that if \mathbf{k} is algebraic over its prime field, then $\sigma \in \text{Aut}(\mathbf{k})$. Conversely, by [5], Chapitre II, §4:

Lemma 6.2. *Let I and J be proper ideals of V with $I \subseteq J$ and let $\sigma \in \text{Aut}(\mathbf{k})$. Then there is exactly one morphism $\phi : V/I \rightarrow V/J$ that induces σ in the above sense; it is given by $\phi(a + I) = \sigma(a) + J$ for all $a \in V$.*

In the next proposition A and B are complete local noetherian rings with maximal ideals \mathfrak{m} and \mathfrak{n} and residue field A/\mathfrak{m} of characteristic $p > 0$.

Proposition 6.3. *Suppose $A/\mathfrak{m} \cong B/\mathfrak{n}$, and A/\mathfrak{m} is algebraic over its prime field. Then any morphism $A \rightarrow B$ is local, and for any $m > 0$ there is an $n > m$ such that any morphism $A_m \rightarrow B_m$ that can be lifted to a morphism $A_n \rightarrow B_n$ can be lifted to a morphism $A \rightarrow B$.*

Proof. Put $\mathbf{k} = A/\mathfrak{m}$, so \mathbf{k} is algebraic over its prime field, and thus perfect. Let $V := W[\mathbf{k}]$ be the ring of Witt vectors over \mathbf{k} . We can assume $A = V[[x]]/I$ and $B = V[[y]]/J$, where

$$I = (f_1, \dots, f_k) \subseteq (p, x)V[[x]], \quad J = (g_1, \dots, g_l) \subseteq (p, y)V[[y]]$$

are ideals, with $x = x_1, \dots, x_d$ and $y = y_1, \dots, y_e$, and where $x_1, \dots, x_d, y_1, \dots, y_e$ are distinct variables. Let $G := \text{Aut}(\mathbf{k})$. Let V_A and V_B be the images of V under the canonical morphisms $V[[x]] \rightarrow A$ and $V[[y]] \rightarrow B$. Suppose $\phi : A \rightarrow B$ is a morphism. Then $\phi(V_A) = V_B$, for example by [5], Chapitre II, §4. Hence ϕ is a local morphism, and ϕ induces on \mathbf{k} an automorphism σ . By Lemma 6.2 the morphism $\phi : A \rightarrow B$ is completely determined by σ and $\phi(x_1 + I), \dots, \phi(x_d + I)$. Conversely, given any $\sigma \in G$ and $z_1, \dots, z_d \in (y)\mathbf{k}[[y]]$, there is a morphism $\phi : A \rightarrow B$ such that

$$\phi \text{ induces } \sigma \text{ and } \phi(x_1 + I) = z_1 + J, \dots, \phi(x_d + I) = z_d + J$$

if and only if $(\sigma f_1)(z_1, \dots, z_d), \dots, (\sigma f_k)(z_1, \dots, z_d) \in J$. The rest of the argument follows the proof of Proposition 4.2, using Proposition 6.1 instead of Proposition 4.1. \square

In particular, we now have Theorem 1.1 in the mixed characteristic case.

7. GABBER'S COUNTEREXAMPLES

Let \mathbf{k} be a field and a_1, a_2, \dots and b_1, b_2, \dots elements of \mathbf{k} such that for each $n > 0$ there is an automorphism of \mathbf{k} sending a_i to b_i for $i = 1, \dots, n$. Define $f, g \in \mathbf{k}[[x, y, z]]$ by $f := \sum_{n=1}^{\infty} a_n z^n$ and $g := \sum_{n=1}^{\infty} b_n z^n$, and define $f_i, g_i \in \mathbf{k}[[x, y, z]]$ for $i = 1, \dots, 5$ by

$$\begin{aligned}
 f_1 = g_1 = x, \quad f_2 = g_2 = y, \quad f_3 = g_3 = y - x, \quad f_4 = g_4 = y - zx, \\
 f_5 = y - fx, \quad g_5 = y - gx.
 \end{aligned}$$

Put $A := \mathbf{k}[[x, y, z]]/(f_1 f_2^2 f_3^3 f_4^4 f_5^5)$ and $B := \mathbf{k}[[x, y, z]]/(g_1 g_2^2 g_3^3 g_4^4 g_5^5)$. (The powers are probably not essential, but they allow us to distinguish branches by multiplicity.) Then A and B are complete local noetherian rings, and the assumptions on \mathbf{k} and (a_n) and (b_n) guarantee that $A_n \cong B_n$ for all $n > 0$. One can show that each isomorphism $A \rightarrow B$ induces an automorphism of $\mathbf{k}[[z]]$ sending z to z and $f(z)$ to $g(z)$. Let $\pi : \mathbf{k}[[z]] \rightarrow \mathbf{k}$ be given by $\pi(\sum c_n z^n) = c_0$ (all $c_n \in \mathbf{k}$), and suppose the following conditions are satisfied:

- (1) there is no automorphism of \mathbf{k} sending a_n to b_n for all $n > 0$;
- (2) there is a subfield \mathbf{k}_0 of \mathbf{k} such that $a_n, b_n \in \mathbf{k}_0$ for all $n > 0$, and the natural inclusion $\mathbf{k}_0 \rightarrow \mathbf{k}[[z]]$ is the only ring morphism $\iota : \mathbf{k}_0 \rightarrow \mathbf{k}[[z]]$ with $\pi \circ \iota = \text{id}_{\mathbf{k}_0}$.

Then A and B are not isomorphic, because any automorphism of $\mathbf{k}[[z]]$ sending z to z and $f(z)$ to $g(z)$ induces on the residue field \mathbf{k} an automorphism sending a_n to b_n for all $n > 0$, violating (1). Here are two ways to realize this idea:

(i) Let p be a prime number, let \mathbf{k} be the perfect closure of $\mathbb{F}_p(a_1, a_2, \dots)$ where a_1, a_2, \dots are algebraically independent over \mathbb{F}_p , and put $b_n := a_{n+1}$. Then all conditions above are satisfied: (2) holds with $\mathbf{k}_0 = \mathbf{k}$ because \mathbf{k} is perfect; see [5].

(ii) Here \mathbf{k} will be a field extension of \mathbb{Q} of transcendence degree 1. Let \mathbf{k}_0 be the Galois extension of \mathbb{Q} generated by the 2^n th roots of 1 and 3, $n > 0$, and choose $\eta_n, a_n \in \mathbf{k}_0$ for $n > 0$ such that η_n is a primitive 2^n th root of unity, $\eta_{n+1}^2 = \eta_n$, $a_1^2 = 3$, $a_{n+1}^2 = a_n$. Let t be transcendental over \mathbf{k}_0 , and put

$$\mathbf{k} := \mathbf{k}_0(t)(\sqrt{t + i + \eta_n^i a_n} : i \in \mathbb{Z}, n > 0).$$

If $\sigma \in \text{Aut}(\mathbf{k})$ and $\sigma(t) = t$, then σ preserves the set of $c \in \mathbf{k}_0$ for which $t + c$ has a square root in \mathbf{k} , and this set is $\{i + \eta_n^i a_n : i \in \mathbb{Z}, n > 0\}$, so σ restricts to the identity on \mathbf{k}_0 . Now \mathbf{k} is countable, so $G := \{\sigma \in \text{Aut}(\mathbf{k}) : \sigma(t) = t\}$ has countable index in $\text{Aut}(\mathbf{k})$, and G has trivial image in $\text{Aut}(\mathbf{k}_0)$ under the restriction map $\text{Aut}(\mathbf{k}) \rightarrow \text{Aut}(\mathbf{k}_0)$, so the image of $\text{Aut}(\mathbf{k})$ under this restriction map is countable. It follows that we can choose b_1, b_2, \dots in \mathbf{k}_0 with $b_1^2 = 3$ and $b_{n+1}^2 = b_n$ for all $n > 0$ such that there is no automorphism of \mathbf{k} sending a_n to b_n for all $n > 0$.

REFERENCES

- [1] S. CUTKOSKY AND H. SRINIVASAN, An intrinsic criterion for isomorphism of singularities, *Am. Journal of Math.* **115** (1993), 789–821. MR1231147 (94h:14005)
- [2] J. DENEFF AND L. LIPSHITZ, Ultraproducts and approximation in local rings. II, *Math. Ann.* **253** (1980), 1–28. MR594530 (82g:13021)
- [3] H. MATSUMURA, *Commutative Algebra*, 2nd edition, Mathematics Lecture Note Series, Benjamin, 1980. MR0266911 (42:1813)
- [4] G. PFISTER AND D. POPESCU, Die strenge Approximationseigenschaft lokaler Ringe, *Inv. Math.* **30** (1975), 145–174. MR0379490 (52:395)
- [5] J-P. SERRE, *Corps Locaux*. Hermann, Paris, 1968. MR0354618 (50:7096)

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS, 1409 W. GREEN STREET, URBANA, ILLINOIS 61801

E-mail address: vddries@math.uiuc.edu